BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet adalah gabungan dari berbagai macam jaringan yang terdiri dari berbagai macam komputer, sistem dan *database*. Untuk bisa mendukung *database* yang berbeda kadang memerlukan perubahan yang cukup besar, untuk keperluan itu maka dicarilah suatu format *database* yang bisa digunakan oleh semuanya tanpa harus melakukan konversi apapun. Melalui XML data bisa diakses oleh komputer apa saja. Semua sistem dan aplikasi bisa mendukungnya, sehingga tercipta *database* yang universal. Pertukaran data antar *database* yang berbeda adalah hal yang sulit dilakukan tetapi jika *database* tersebut berformat XML maka itu menjadi suatu hal yang mudah.

Semakin luasnya penggunaan XML pada berbagai layanan di internet, maka mulai muncul permasalahan mengenai kebutuhan akan keamanan data bagi informasi yang terkandung didalam sebuah dokumen XML. Hal ini mengingat bahwa sebuah XML hanya tersusun dari sekumpulan teks yang sangat mudah untuk dipahami oleh pengguna atau program komputer.

Salah satu cara yang digunakan untuk menjamin keamanan data XML adalah dengan menyandikan data menjadi suatu kode-kode yang tidak dimengerti, atau dengan kata lain, sehingga apabila ada orang yang tidak berhak atas data tersebut, akan sulit untuk mengetahui isi data yang sebenarnya.

Oleh karena itu, dibutuhkan suatu algoritma kriptografi untuk menyandikan data XML, salah satunya algoritma Rivest Shamir Adleman *(RSA)*. RSA banyak digunakan oleh berbagai jenis produk, *platform*, dan industri di seluruh bagian dunia. Seorang penyerang biasanya memecahkan RSA dengan memfaktorkan modulus publik ke dalam dua buah faktor prima. Keamanan RSA tergantung pada kesulitan dalam memfaktorkan modulus, juga pada besarnya kunci yang dipilih untuk menyandikan. Perkembangan perangkat lunak saja tidak akan membuat RSA menjadi lemah, selama digunakan panjang kunci yang sesuai, untuk itu penulis mengambil judul skripsi "Implementasi Algoritma *Rivest Shamir Adleman* (RSA) Untuk Penyandian Data *Extensible Markup Language* (XML)".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah dalam skripsi ini adalah bagaimana caranya mengimplementasikan algortima RSA untuk keamanan dan kerahasiaan data XML?

1.3 Batasan Masalah

Batasan masalah pada skripsi ini adalah:

a. Penyandian data diterapkan hanya pada isi tag elemen XML, bukan seluruh dokumen XML.

b. Implementasi algoritma RSA ditujukan pada saat data disimpan dalam

XML, bukan pada saat XML diproses melalui internet.

c. Data yang disandikan hanya dalam format teks.

d. Pada skripsi ini tidak dibahas bagaimana sulitnya memecahkan algoritma RSA.

e. Dalam skripsi ini digunakan analisis dan perancangan sistem berorientasi objek.

1.4 Tujuan

Penelitian ini bertujuan untuk:

a. Mengetahui apakah algoritma RSA dapat diimplementasikan pada data XML.

b. Memberikan salah satu solusi untuk masalah keamanan dan kerahasiaan data pada XML.

1.5 Metodologi Penelitian

Metodologi penelitian pada skripsi ini, penulis melakukan studi literatur dari beberapa jurnal, *handout* dan artikel mengenai tinjauan keamanan XML, mengapa XML perlu diamankan dan seberapa amankah algoritma RSA jika digunakan untuk penyandian data.

1.6 Teknik Pengumpulan Data

Teknik pengumpulan data pada skripsi ini, penulis mencari beberapa sumber dari buku, *e-book,* artikel, jurnal, situs internet dan *handout* yang terkait dengan XML dan algoritma RSA.

1.7 Sistematika Penulisan Skripsi

BAB I Pendahuluan

Bab I berisi latar belakang, rumusan masalah, batasan masalah, tujuan, metodologi penelitian, teknik pengumpulan data dan sistematika penulisan skripsi.

BAB II Dasar Teori

Bab II berisi beberapa teori yang mendasari penyusunan skripsi.

BAB III Analisis dan Perancangan

Bab III berisi analisis dan perancangan dari algoritma RSA yang akan diterapkan.

BAB IV Implementasi dan Pengujian

Bab IV berisi implementasi dan pengujian dari algoritma RSA ke dalam XML.

BAB V Penutup

Bab V berisi kesimpulan dan saran dari hasil penelitian yang dilakukan.

Daftar Pustaka

Lampiran